1073 AF

Docket No.: 64965-017 PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of :

William LO :

Serial No.: 09/170,221 : Group Art Unit: 2631

Filed: October 13, 1997 : Examiner: Kevin M. Burd

For: APPARATUS AND METHOD FOR SECURE MEDIA INDEPENDENT INTERFACE COMMUNICATIONS BY CORRUPTING TRANSMIT DATA ON SELECTED REPEATER PORT

TRANSMITTAL OF APPEAL BRIEF

Commissioner for Patents
Washington, DC 20231

Sir:

Submitted herewith in triplicate is Appellant(s) Appeal Brief in support of the Notice of Appeal filed December 9, 2002. Please charge the Appeal Brief fee of $320.00 to Deposit Account 500417.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 500417 and please credit any excess fees to such deposit account.

Respectfully submitted,

MCDERMOTT, WILL & EMERY

Edward J. Wise
Registration No. 34,523

600 13th Street, N.W.
Washington, DC 20005-3096
(202) 756-8628 EJW:khb
Date: January 6, 2003
Facsimile: (202) 756-8087

TABLE OF CONTENTS

Docket No.: 64965-017 PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of :

William LO :

Serial No.: 09/170,221 : Group Art Unit: 2631

Filed: October 13, 1997 : Examiner: Kevin M. Burd

For: APPARATUS AND METHOD FOR SECURE MEDIA INDEPENDENT INTERFACE COMMUNICATIONS BY CORRUPTING TRANSMIT DATA ON SELECTED REPEATER PORT

APPEAL BRIEF

Commissioner for Patents
Washington, DC 20231

Sir:

This Appeal Brief is submitted in support of the Notice of Appeal filed November , 2002.

I. REAL PARTY IN INTEREST

The real party in interest is Advanced Micro Devices, Inc.

II. RELATED APPEALS AND INTERFERENCES

Appellant are unaware of any related appeals or interferences.

01/07/2003 CNGUYEN 00000007 500417 09170221
01 FC:1402 320.00 CH

01/08/2003 CNGUYEN 00000013 500417 09170221
01 FC:1402 320.00 CH

III. STATUS OF CLAIMS

Claims 7-11 and 16-19 are pending in this application. Claims 7-11 and 16-19 have been finally rejected. It is from the final rejection of claims 7-11 and 16-19 that this Appeal is taken.

IV. STATUS OF AMENDMENTS

No Amendment has been submitted subsequent to the issuance of the final Office Action dated September 9, 2002. A Response Under 37 CFR 1.116 (Request for Reconsideration) was submitted on September 26, 2002. According to the Advisory Action dated October 8, 2002, the Response was considered, but the Examiner adhered to the rejections imposed in the September 9, 2002 Final Office Action.

However, an Amendment Under 37 CFR 1.116 was submitted with filing the Notice of Appeal, correcting obvious editorial errors in the specification. As no new matter has been entered, it is presumed that the amendments to the specification have been entered.

V. SUMMARY OF THE INVENTION

Figure 1 is a diagram illustrating a conventional repeater network. The network 10 includes a repeater 12 configured for transmitting a data packet received on an input port to the other ports for reception by respective network nodes 14. For example, assume that node (i.e., workstation) 14a transmits a data packet via the network medium 16. The transmitted data packet is received by a physical layer transceiver (PHY) 20a that recovers the digital data from the transmitted analog signal. As recognized in the art, the PHY transceiver 20a may be a 100 Base-TX IEEE standard 802.3u receiver, configured for receiving a 3-level MLT-3 encoded analog signal at a 125 Megabit per second rate, and configured for output of the transmit data as

nibble-wide (4 bits) or byte-wide transmit data (TXD) to the MII 18 that connects between the PHY 20a and the repeater 12.

The repeater 12, upon receiving the transmit data from the PHY transceiver 20a, retransmits the transmit data to all the other ports for transmission by the other PHY transceivers (e.g., 20b, 20c and 20d). The network stations 14 of the other ports will ignore the packet unless the destination address of the packet matches the network stations own address. One problem with this arrangement is that any network node can eavesdrop on all packets that are transmitted on the network. Hence, an unauthorized workstation 14e may eavesdrop on all data packets by obtaining access to a repeater port.

Newer repeater architectures have proposed reducing the number of pins on the repeater core by bussing common signals such as the MII transmit data (TXD [3:0]), receiver data (RXD [3:0]), receive clock (RX_CLK), receive data valid (RX_DV), and receive error (RX_ER) signals. These pins can be shared because only one port should be sourcing data at any given time. If more than port sources data then there is a collision, and the actual data that are sourced is a don't-care situation.

The bussing of MII signals, however, further reduces the ability to individually control the data which is transmitted on each port, such that each port of the repeater 12 transmits either valid data when TX_EN is asserted, or does not transmit any data at all. Hence, an unauthorized workstation 14e can more effectively eavesdrop on all data packets by obtaining access to the bussed RXD signal path.

The present invention address this problem in the conventional repeater network of an unauthorized workstation eavesdropping on all data packets by obtaining access to a repeater

port by ***corrupting network data*** on repeater ports that do not serve the destination network node of a given data packet.

Claim 16 is presented below with elements read on the specification and drawings.

A repeater system comprising:

repeater ports (34a, 34b...; Figure 2; page 5, lines 7-19; page 6, lines 8-13) for communication with respective network nodes (14 (a-e); Figure 1; page 5, lines 7-12) via respective repeater media independent interfaces (40; Figure 2; page 5, lines 9-19); and

a repeater core (32; Figure 2; page 7, lines 8-32) comprising:

(1) a table for identifying each network node by its corresponding destination address and the corresponding repeater port (44; Figure 2; page 5, lines 20-25), and

(2) a security circuit for transmitting a data packet on an identified one of the repeater ports corresponding to the network node having the destination address specified in the data packet (46; Figure 2; page 5, lines 28-32), the security circuit corrupting transmission of the data packet on other of the repeater ports corresponding to network nodes not having the destination address specified in the data packet by concurrently asserting a transmit error signal and deasserting a transmit enable signal on the respective media independent interfaces (46; Figure 2; page 5, line 33 through page 6, line 15).

VI. ISSUES

A. The Rejections:

(1) Claims 7-11 and 16-19 stand finally rejected under 35 U.S.C. § 102(e) as being anticipated by Hayakawa.

(2) Claims 7-11 and 16-19 stand finally rejected under 35 U.S.C. § 102(e) as being anticipated by Judd [et al.].

B. The Issues Which arise in this Appeal and require resolution by the Honorable Board of Patent Appeals and Interferences (the Board) are:

(1) Whether claims 7-11 and 16-19 are unpatentable under 35 U.S.C. § 102 for lack of novelty, as evidenced by Hayakawa; and

(2) Whether claims 7-11 and 16-19 are unpatentable under 35 U.S.C. § 102 for lack of novelty, as evidenced by Judd [et al].

VII. GROUPING OF CLAIMS

The appealed claims do not stand or fall together as a group. Appellant separately argues the patentability of each claim.

VIII. THE ARGUMENT

Independent claim 7 is directed a method of transmitting a (actual) data packet received by a repeater from a transmitting network node on a corresponding repeater port. The method comprising, *inter alia*, identifying one of a plurality of repeater ports serving a destination network node. This identification is made based on a destination address in the data packet received by the repeater from the transmitting network node. The repeater port serving the destination network node (for the data packet) transmits the (actual) data packet by concurrently asserting (with the transmitting of the (actual) data packet on the media independent interface corresponding to that repeater port) a transmit enable signal on the ***media independent interface***

(emphasis added) corresponding to that repeater port. For the other repeater ports (that are not serving the destination network node), there is a step of corrupting transmission of the data packet which is accomplished by concurrently asserting a transmit error signal and deasserting the transmit enable signal on the media independent interfaces that correspond to the other repeater ports.

Independent claim 16 is directed to a repeater system comprising repeater ports for communication with respective network nodes via respective repeater ***media independent interfaces*** (emphasis added) and a repeater core. The repeater core has (1) a table for identifying each network node by its corresponding destination address and the corresponding repeater port, and (2) a security circuit for transmitting a data packet on an identified one of the repeater ports corresponding to the network node having the destination address specified in the data packet. The security circuit corrupts transmission of the data packet on other of the repeater ports corresponding to network nodes not having the destination address specified in the data packet by concurrently asserting a transmit error signal and deasserting a transmit enable signal on the respective media independent interfaces.

The pivotal issued generated by the imposed rejection under 35 U.S.C. §102 is whether the Examiner has discharged the initial burden of identifying wherein each of Hayakawa and Judd [et al.] identically describes each and every step/element of the claimed invention. It is Appellant's position that the Examiner has not identified wherein each of Hayakawa and Judd [et al.] identically describes the claimed method/system, either expressly or under the doctrine of inherency. ***In re Rijckaert***, 9 F.3d 1531, 28 USPQ2d 1955 (Fed. Cir. 1993; ***Lindemann Maschinenfabrik GMBH v. American Hoist & Derrick Co.***, 730 F.2d 1452, 221 USPQ 481 (Fed. Cir. 1984).

The Examiner's Approach

The Examiner's attempt to identify where the features of claims 7-11 and 16-19 are found in Hayakawa is found on pages 3 and 4 of the September 9, 2002 Final Office Action under item 6, and consist of the following:

> Regarding claims 7-9, 11, 16 and 17, Hayakawa discloses a method of transmitting and receiving data. An error is detected in the received data (asserting a transmit error). When this occurs, receiving the data stops since there are errors present (deasserting a transmit enable). Following these steps, a request for retransmission is sent from the receiving apparatus. The data pattern of the request for retransmission will be known to all elements of the system. See column 13, lines 7-16 for details of the requirements for the request for retransmission to be sent. Data is transmitted throughout the system shown in figure 2. It is inherent that the data transmission has a destination address otherwise the data would not be received in its proper destination.
>
> Regarding claim 10, the receiver will enter an idle state immediately after sending the request for retransmission since no data is to be received at this instant time.
>
> Regarding claims 18 and 19, Hayakawa discloses the transmission node respond to each of the retransmission requests in the system (column 13, lines 7-16).

The Examiner's attempt to identify where the features of claims 7-11 and 16-19 are found in Judd [et al.] is found on pages 4 and 5 of the September 9, 2002 Final Office Action under item 7, and consist of the following:

> Regarding claims 7-9, 11, 16 and 17, Judd discloses a method of transmitting and receiving data. An error is detected in the received data (asserting a transmit error). When this occurs, receiving the data stops since there are errors present (deasserting a transmit enable). Following these steps, a request for retransmission is sent from the receiving apparatus. The data pattern of the request for retransmission will be known to all elements of the system. See column 1, lines 49-65 for details of the requirements for the request for retransmission to be sent. Data is transmitted throughout the system as shown in figures 3-5. The transmission data has a address field as shown in figures 6A and 6B.
>
> Regarding claim 10, the receiver will enter an idle state immediately after sending the request for retransmission since no data is to be received at this instant time.

Regarding claims 18 and 19, Judd discloses the multiple paths from a transmitting node to a receiving node exist so a plurality of transmissions are sent (column 1, lines 66 to column 2, line 8).

Appellants' Position

Appellant submits that the Examiner did not discharge the initial burden of establishing a *prima facie* basis to deny patentability to the claimed invention under 35 U.S.C. §102 for lack of novelty. Specifically, neither Hayakawa nor Judd [et al.] is directed to a repeater or repeater system. What is being done in Hayakawa and Judd is substantially different from what is being done in the present invention, as represented by independent claims 7 and 16, and, in fact, has nothing to do with the present invention.

More specifically, the present invention addresses a problem of conventional repeaters wherein an unauthorized workstation can eavesdrop on all data packets being transmitted by the repeater by obtaining access to a repeater port. This problem is addressed in the present invention by an arrangement for secure repeater communications to network nodes where the (actual) data packet received by the repeater from a transmitting network node is transmitted from the repeater port(s) serving the destination network node for that received data packet, and a corrupted data (data that is intentionally not an actual data packet) is transmitted from repeater ports that do not serve the destination network node of the given data packet.

Hence, in the present invention, once a repeater port corresponding to the network node having the destination address specified in the received data packet is identified, the (actual) received data packet is transmitted on the identified repeater port by ***asserting***, on the media independent interface corresponding to the identified repeater port, ***the transmit enable signal*** (TX_EN for the respective network port that has the destination address specified in the received data packet) ***concurrently with transmitting the received data packet***, also on the media

independent interface corresponding to the identified repeater port. In addition, corrupt data (data that is intentionally not the actual data packet) is transmitted on repeater ports that correspond to network nodes that do not have the destination address specified in the data packet. This is carried out by concurrently asserting the transmit error signal (TX_ER) and deasserting the transmit enable signal (TX_EN) on the respective media independent interfaces (for the respective network ports that do not have the destination address specified in the data packet). Independent claims 7 and 16 both have these features.

These features, however, are simply not disclosed or suggested in Hayakawa or Judd [et al.]. This is quite understandable since, as noted above, what is being done in Hayakawa and Judd is substantially different from what is being done in the present invention. Both Hayakawa and Judd are concerned with addressing transmission errors, which the present invention is not.

More specifically, in Hayakawa, when a reception node (of a receiving network device) determines that there has been a reception error, the reception node issues a re-transmission request of data to the transmitting node (of the distinct transmitting network device). The nodes in Hayakawa are clearly not ports of a repeater, as is required in the present claims. A repeater is the simplest type of LAN interconnection device. A repeater moves all received packets or frames between LAN segments (the nodes in Hayakawa), and its primary function is to extend the length of the network media. A repeater is not a destination, as is the case for the nodes of Hayakawa.

Furthermore, there is nothing in Hayakawa, let alone at column 13, lines 7-16, that discloses or suggests anything about "corrupting transmission of the data packet on other repeater ports", which is clearly an intentional act. More specifically, "corrupting transmission of the data packet on other repeater ports" is done by concurrently asserting a transmit error

signal and deasserting the transmit enable signal ***on the media independent interfaces*** (emphasis added) corresponding to the other repeater ports", as recited in claim 7, or with "a security circuit for transmitting a data packet on an identified one of the repeater ports corresponding to the network node having the destination address specified in the data packet, ***the security circuit corrupting transmission of the data packet on other of the repeater ports*** (emphasis added) corresponding to network nodes not having the destination address specified in the (received) data packet by concurrently asserting a transmit error signal and deasserting a transmit enable signal ***on the respective media independent interfaces***" (emphasis added), as recited in claim 16. Issuing a re-transmission request of data to the transmitting node, as is done in Hayakawa, is a completely different, and unrelated function. Furthermore, Appellant does not see, and the Examiner has not identified where in Hayakawa there is specifically disclosed [a] media independent interface(s) (MIIs), which are required in the claims. The connections shown in FIGS. 2 and 3 are the actual media that connects nodes in a communication system, not MIIs.

In Judd [et al.], an error recovery system/method is disclosed. More specifically, Judd [et al.] are concerned with recovering from errors occurring during transmission of data between (distinct network) nodes. The dual port node 10 shown in FIG. 1 of Judd [et al.] is clearly not a repeater, as it can be the destination of an inbound frame. A repeater is never the destination of an inbound frame. The fact that dual port node 10 can function to forward an inbound frame to an outbound line of another port does not make the dual port node 10 a repeater. Even if the function of dual port node 10 in forwarding of an inbound frame to an outbound line of another port is similar to the actual functioning of a repeater, the Examiner has not established that the arrangement of Judd [et al.] would ever suffer the problem of a conventional repeater wherein an unauthorized workstation can eavesdrop on all data packets being transmitted by the repeater by

obtaining access to a repeater port. Given the more sophisticated architecture of dual port node 10, and the fact that such dual port node will typically be an electronic device such as a computer, printer, storage device, etc. (see column 3, lines 63-65), this does not appear to be the case.

There is nothing in Judd [et al.], let alone at column 1, lines 49-65, that discloses or suggests anything about "corrupting transmission of the data packet on other repeater ports" (which is clearly intentional) by concurrently asserting a transmit error signal and deasserting the transmit enable signal ***on the media independent interfaces*** (emphasis added) corresponding to the other repeater ports", as recited in claim 7, or with "a security circuit for transmitting a data packet on an identified one of the repeater ports corresponding to the network node having the destination address specified in the data packet, ***the security circuit corrupting transmission of the data packet on other of the repeater ports*** (emphasis added) by concurrently asserting a transmit error signal and deasserting a transmit enable signal ***on the respective media independent interfaces***" (emphasis added), as recited in claim 16. The Examiner cannot ignore the fact that the present claims are directed to a repeater or repeater system.

In the operations described in each of Hayakawa and Judd [et al.], data is being transmitted ***between ports of distinct network devices*** (i.e., network nodes). Neither Hayakawa nor Judd [et al.] is concerned with what is being transmitted from different ports of a repeater or repeater system, as in the present invention, since neither Hayakawa nor Judd [et al.] discloses or suggests a repeater having a repeater (transmission) port corresponding to the network node having the destination address specified in a (received) data packet from which the (actual) received data packet is transmitted to the specified address, and another repeater port

corresponding to a network node that does not have the destination address specified in the received data packet from which corrupted data is (intentionally) transmitted.

Furthermore, in the present invention, there is nothing disclosed about determining that the data transmitted by the ports, corresponding to a network node that do not have the destination address specified in the (received) data packet, are in fact corrupted data, or determining data that is in error, as is the case in Hayakawa and Judd [et al.]. Clearly, the corrupted data being transmitted by the port(s) corresponding to a network node(s) that do not have the destination address specified in the (received) data packet, is not error data in terms of what is disclosed in both Hayakawa and Judd [et al.], as the transmission of the corrupted data is intentional in the present invention.

Certainly, the present invention does not ever envision issuing of a re-transmission request of data to the transmitting node, as is disclosed in Hayakawa, when the data being transmitted by the ports corresponding to a network node that do not have the destination address specified in the (received) data packet is corrupted, as the corrupted data being transmitted by these ports is not intended for any destination node. Similarly, the present invention does ever envision error recovery, as is disclosed in Judd [et al.], when the data being transmitted by the ports corresponding to a network node that do not have the destination address specified in the (received) data packet is corrupted, as the corrupted data being transmitted by these ports is (again) not intended for any destination node. This is consistent with the objective of the present invention in not allowing an unauthorized workstation to eavesdrop on all (real/uncorrupted) data packets by obtaining access to a repeater port, and this is accomplished by transmitting corrupted data from the repeater ports that do not serve the destination network node of the received data

packet. This is not an objective of either Hayakawa or Judd [et al.], let alone being disclosed in these references as something to be addressed.

Frankly, the Examiner's analysis of the rejected claims, vis-à-vis, Hayakawa and Judd [et al.], evinces that the Examiner may not understand the present invention, or does not wish to read the claimed limitations in the specific manner in which they are recited. Clearly, the claimed limitations are of sufficient specificity to be clearly distinguishable from that which is disclosed in Hayakawa and Judd [et al.].

Dependent claims

It is not apparent, and the Examiner has not properly identified wherein each of Hayakawa and Judd [et al.] discloses or suggests a method of transmitting a data packet, as recited in claim 7, further comprising receiving by ***a physical layer transmitter*** (emphasis added) the transmit data, the deasserted transmit enable signal, and the asserted transmit error signal from at least one of the ***media independent interfaces*** (emphasis added) corresponding to at least one of the ***other repeater ports*** (emphasis added), and ***selectively transmitting a prescribed data pattern as corrupted transmit data from the physical layer transmitter*** (emphasis added) to at least one of the network nodes corresponding to the at least one of the other repeater ports ***based on the received transmit data, the deasserted transmit enable signal, and the asserted transmit error signal*** (emphasis added), as recited in claim 8.

It is not apparent, and the Examiner has not properly identified wherein each of Hayakawa and Judd [et al.] discloses or suggests in a method of transmitting a data packet, as recited in claim 8, wherein the selectively transmitting step includes ***detecting a predetermined condition in the transmit error signal and the transmit enable signal*** (e.g., the flow from state 60 to state 62 to

state 64 shown in Figure 4 of the present application), the selectively transmitting step outputting the prescribed data pattern (see corrupted data generator 72 of Figure 5 of the present application) in response to the concurrent detection of the asserted transmit error signal and the deasserted transmit enable signal contiguously following the predetermined condition (states 66 and 68 of Figure 4 of the present application), as recited in claim 9.

It is not apparent, and the Examiner has not properly identified wherein each of Hayakawa and Judd [et al.] discloses or suggests in a method of transmitting a data packet, as recited in claim 9, wherein the step of detecting the predetermined condition comprises first detecting, contiguously following an idle state (state 60 shown in Figure 4 of the present application), a concurrent assertion of the transmit enable signal and deassertion of the transmit error signal for at least a first predetermined number of cycles (i.e., the flow from state 60 to state 62 to state 64 shown in Figure 4 of the present application), as recited in claim 10.

It is not apparent, and the Examiner has not properly identified wherein each of Hayakawa and Judd [et al.] discloses or suggests a method of transmitting a data packet, as recited in claim 8, further comprising ***selecting the predetermined data pattern based on an identified physical layer protocol between the destination network node and the physical layer transmitter***, (emphasis added) (see, page 8, line 28 through page 9, line 2), as recited in claim 11.

Furthermore, it is not apparent, and the Examiner has not properly identified wherein each of Hayakawa and Judd [et al.] discloses or suggests a repeater system, as recited in claim 16, further comprising at least one ***physical layer transceiver*** (emphasis added) for receiving the transmitted data packet, the transmit error signal, and the deasserted transmit enable signal for at least one of the ***media independent interfaces*** (emphasis added) corresponding to the other of the network ports, the physical layer transceiver ***outputting a prescribed data pattern as a corrupted data***

packet based on the concurrent assertion of the transmit error signal and the deassertion of the transmit enable signal, (emphasis added), as recited in claim 17.

It is not apparent, and the Examiner has not properly identified wherein each of Hayakawa and Judd [et al.] discloses or suggests in a repeater system, as recited in claim 17, wherein the ***physical layer transceiver outputs a modified transmit enable signal, a modified transmit error signal and the corrupted data packet to a second media independent interface*** (emphasis added) (see physical layer transceiver (PHY) 36 of Figure 3 and transmit output circuitry 70 of Figure 5) for transmission to the corresponding network node based on the concurrent assertion of the transmit error signal and the deassertion of the transmit enable signal, as recited in claim 18.

Finally, it is not apparent, and the Examiner has not properly identified wherein each of Hayakawa and Judd [et al.] discloses or suggests in a repeater system, as recited in claim 17, wherein the ***physical layer transceiver*** (emphasis added) includes a detection circuit for detecting a predetermined condition in the transmit error signal and the transmit enable signal, the ***physical layer transceiver*** (emphasis added) outputting the ***corrupted data packet*** (emphasis) in response to the concurrent detection of the asserted transmit error signal and the deasserted transmit enable signal contiguously following the predetermined condition, as recited in claim 19.

Based upon the foregoing, Appellant respectfully submit that the Examiner did not discharge initial burden of establishing a *prima facie* basis to deny patentability to the claimed invention under 35 U.S.C. § 102 for lack of novelty.

IX. PRAYER FOR RELIEF

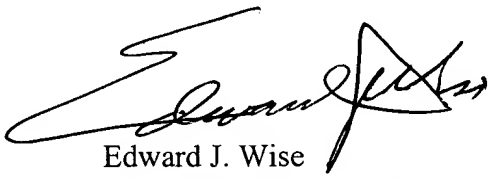
Based upon the arguments submitted supra, Appellant respectfully submit that both Hayakawa and Judd [et al.] do not identically describe the claimed invention within the meaning

of 35 U.S.C. §102, either expressly or under the doctrine of inherency. Appellant, therefore, respectfully solicits the Honorable Board to reverse the Examiner's rejection of claims 7-11 and 16-19 under 35 U.S.C. § 102 for lack of novelty as evidence by either Hayakawa or Judd [et al.].

To the extent necessary, a petition for an extension of time under 37 CFR § 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 500417 and please credit any excess fees to such deposit account.

Respectfully submitted,

MCDERMOTT, WILL & EMERY



Edward J. Wise
Registration No. 34,523

600 13th Street, N.W.
Washington, DC 20005-3096
(202) 756-8628 EJW:
Date: January 6, 2003
Facsimile: (202) 756-8087

APPENDIX

7. A method of transmitting a data packet received by a repeater from a transmitting network node on a corresponding repeater port, the method comprising:

identifying one of a plurality of repeater ports serving a destination network node based on a destination address in the data packet;

transmitting the data packet on the one repeater port serving the destination network node by concurrently asserting a transmit enable signal on a corresponding media independent interface; and

corrupting transmission of the data packet on other repeater ports by concurrently asserting a transmit error signal and deasserting the transmit enable signal on the media independent interfaces corresponding to the other repeater ports.

8. The method of claim 7, further comprising:

receiving by a physical layer transmitter the transmit data, the deasserted transmit enable signal, and the asserted transmit error signal from at least one of the media independent interfaces corresponding to at least one of the other repeater ports; and

selectively transmitting a prescribed data pattern as corrupted transmit data from the physical layer transmitter to at least one of the network nodes corresponding to the at least one of the other repeater ports based on the received transmit data, the deasserted transmit enable signal, and the asserted transmit error signal.

9. The method of claim 8, wherein the selectively transmitting step includes detecting a predetermined condition in the transmit error signal and the transmit enable signal, the selectively transmitting step outputting the prescribed data pattern in response to the concurrent detection of the asserted transmit error signal and the deasserted transmit enable signal contiguously following the predetermined condition.

10. The method of claim 9, wherein the step of detecting the predetermined condition comprises first detecting, contiguously following an idle state, a concurrent assertion of the transmit enable signal and deassertion of the transmit error signal for at least a first predetermined number of cycles.

11. The method of claim 8, further comprising selecting the predetermined data pattern based on an identified physical layer protocol between the destination network node and the physical layer transmitter.

16. (Amended) A repeater system comprising:

repeater ports for communication with respective network nodes via respective repeater media independent interfaces; and

a repeater core comprising:

(1) a table for identifying each network node by its corresponding destination address and the corresponding repeater port, and

(2) a security circuit for transmitting a data packet on an identified one of the repeater ports corresponding to the network node having the destination

address specified in the data packet, the security circuit corrupting transmission of the data packet on other of the repeater ports corresponding to network nodes not having the destination address specified in the data packet by concurrently asserting a transmit error signal and deasserting a transmit enable signal on the respective media independent interfaces.

17. The system of claim 16, further comprising at least one physical layer transceiver for receiving the transmitted data packet, the transmit error signal, and the deasserted transmit enable signal for at least one of the media independent interfaces corresponding to the other of the network ports, the physical layer transceiver outputting a prescribed data pattern as a corrupted data packet based on the concurrent assertion of the transmit error signal and the deassertion of the transmit enable signal.

18. The system of claim 17, wherein the physical layer transceiver outputs a modified transmit enable signal, a modified transmit error signal and the corrupted data packet to a second media independent interface for transmission to the corresponding network node based on the concurrent assertion of the transmit error signal and the deassertion of the transmit enable signal.

19. The system of claim 17, wherein the physical layer transceiver includes a detection circuit for detecting a predetermined condition in the transmit error signal and the transmit enable signal, the physical layer transceiver outputting the corrupted data packet in response to the concurrent detection of the asserted transmit error signal and the deasserted transmit enable signal contiguously following the predetermined condition.